

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being submitted *via* the USPTO EFS Filing System on the date shown below to **Mail Stop Appeal Brief - Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: October 6, 2006/Jessica Sexton/

Jessica Sexton

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Appellant(s): Narayanan Ganapathy

Examiner: Brandon S. Hoffman

Serial No: 09/771,734

Art Unit: 2136

Filing Date: January 29, 2001

Title: SYSTEM AND METHOD TO FACILITATE SECURE COMMUNICATION OF
DATA

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Appellant's representative submits this brief in connection with an appeal of the above-identified patent application. Payment is being submitted via credit card in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP185USB].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellant, appellant's legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-34 stand rejected by the Examiner. The rejection of claims 1-34 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No amendments were made after the Final Office Action dated May 8, 2006.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))**A. Independent Claim 1**

Independent claim 1 recites a system to facilitate secure communication, comprising: a communication component operative to store an outgoing message received directly from an associated process, the outgoing message including a message key having a key value, an attribute being associated with the communication component, the attribute having selectable attribute conditions that are inaccessible by the associated process; and a filter associated with the communication component, the filter controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions. (*See e.g.*, page 5, line 20 – page 6, line 17; page 9, lines 23-page 10, line 24; page 18, line 18 – page 19, line 11; page 20, lines 1-29)

B. Independent Claim 12

Independent claim 12 recites a system to facilitate secure communication between at least two processes, comprising: a first queue operative to store a request received directly from a first

of the at least two processes and, upon validation of the stored request, to send the stored request to a second of the at least two processes, the stored request including a destination address and a key having a key value; and an interface operative to validate the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the first queue, the at least one key value associated with the first queue being unavailable to the first process. (*See e.g.*, page 5, line 20 – page 6, line 17; page 8, lines 14-25; page 9, lines 23-page 10, line 24)

C. Independent Claim 21

Independent claim 21 recites a system to facilitate secure communication between at least two user-level processes, comprising:

storage means for storing an outgoing message received from a first of the at least two processes, the outgoing message including a message key associated with a destination, an attribute being associated with the storage means, the attribute having selectable attribute conditions unavailable to user-level processes; and (*See e.g.*, page 12, line 21 – page 12, line 18; page 8)

control means for controlling sending of the stored outgoing message from the storage means based on the message key and one of the attribute conditions. (*See e.g.*, page 13, line 19 – page 14, line 8)

D. Independent Claim 25

Independent claim 25 recites a system to facilitate secure communication between at least two user-level processes, comprising:

storage means for storing a request received directly from a first of the at least two processes and, upon validation of the stored request, for sending the stored request to a second of the at least two processes, the stored request including a key having a key value; and (*See e.g.*, page 12, line 21 – page 12, line 18; page 8)

validation means for validating the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the storage means, the at least one key value associated with the storage means being unavailable to user-level processes. (*See e.g.*, page 13, line 19 – page 14, line 8)

E. Independent Claim 28

Independent claim 28 recites a computer-readable medium having computer-executable instructions for: storing in a storage device an outgoing message received directly from an associated user-level process, the outgoing message including a message key having a key value, an attribute being associated with the storage device, the attribute having selectable attribute conditions unavailable to user-level processes; and controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions. (*See e.g.*, page 5, line 20 – page 6, line 17; page 9, lines 23–page 10, line 24; page 18, line 18 – page 19, line 11; page 20, lines 1–29)

F. Independent Claim 29

Independent claim 29 recites a computer-readable medium having computer-executable instructions for: storing a request received directly from a first of at least two user-level processes in a storage device; upon validation of the stored request, sending the stored request to a second of the at least two processes, the stored request including a key having a key value; and validating the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the storage device, the at least one key value associated with the storage device being unavailable to user-level processes. (*See e.g.*, page 5, line 20 – page 6, line 17; page 9, lines 23–page 10, line 24; page 18, line 18 – page 19, line 11; page 20, lines 1–29)

G. Independent Claim 30

Independent claim 30 recites a method to facilitate secure communication from a first user-level process in a system in which the first process is operable to communicate directly with hardware, comprising: storing an outgoing message received directly from the first process in an associated storage device, the outgoing message including a message key having a key value; and controlling sending of the stored message to a second process based on the value of the message key relative to a predetermined at least one key value associated with the storage device, the at least one key value associated with the storage device being unavailable to the first process. (*See e.g.*, page 5, line 20 – page 6, line 17; page 9, lines 23–page 10, line 24; page 18, line 18 – page 19, line 11; page 20, lines 1–29)

H. Independent Claim 34

Independent claim 34 recites a method to facilitate secure communication from a first user-level process in a system in which the first process is operable to communicate directly with hardware, comprising: storing an outgoing message received directly from the first process in a storage device associated with the first process, the outgoing message including a message key associated with a destination, an attribute being associated with the storage device, the attribute having selectable attribute conditions being inaccessible by user-level processes; and controlling sending of the stored outgoing message from the storage device based on the message key of the stored outgoing message and one of the attribute conditions of the storage device. (*See e.g.*, page 5, line 20 – page 6, line 17; page 9, lines 23-page 10, line 24; page 18, line 18 – page 19, line 11; page 20, lines 1-29)

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1, 2, 5-11 and 21-24, 28, 34 are unpatentable under 35 U.S.C. §102(b) over Tucker *et al.* (U.S. 5,808,911).

B. Whether claims 12-15, 20, 25-27 and 29-33 are unpatentable under 35 U.S.C. §102(b) over Tucker *et al.* (U.S. 5,808,911).

C. Whether claims 3, 4 and 16-19 are unpatentable under 35 U.S.C. §103(a) over Tucker *et al.* (U.S. 5,808,911) in view of Neal *et al.* (U.S. 6,766,467).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))**A. Rejection of Claims 1, 2, 5-11 and 21-24, 28, 34 Under 35 U.S.C. §102(b)**

Claims 1, 2, 5-11 and 21-24, 28, 34 stand rejected under 35 U.S.C. §102(b) as being anticipated by Tucker *et al.* (U.S. Patent No. 5,808,911). It is respectfully submitted that this rejection should be reversed for at least the following reasons. Tucker *et al.* does not teach each and every element of the subject invention as recited in the subject claims.

A single prior art reference anticipates a patent claim only if it expressly or inherently describes each and every limitation set forth in the patent claim. *Trintec Industries, Inc., v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 U.S.P.Q.2D 1597 (Fed. Cir. 2002); *See*

Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the ... claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The subject invention relates to providing secure communication of messages from a user-level application or process that has direct access to communication hardware components. Appellant's claimed invention employs message keys that are included in each outgoing message and attributes associated with the communication components to verify authenticity of messages and secure the communications. The attribute conditions associated with the communication component are not accessible by user level processes to ensure the security of the communication system. The attribute and the message key are two distinct security features - the selectable attribute conditions can be used to interpret how the message key is to be used for security. For example, if the attribute has a first condition, the message key may be interpreted in a first manner for security, and if the attribute has a second condition, then the message key may be interpreted in a second manner for security. In particular, independent claim 1 (and similarly independent claims 21, 28 and 34) recites, *a communication component operative to store an outgoing message received directly from an associated process, **the outgoing message including a message key having a key value**, an attribute being associated with the communication component, the attribute having selectable attribute conditions that are inaccessible by the associated process; and a filter associated with the communication component, the filter controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions.*

Tucker *et al.* does not teach or suggest the aforementioned novel aspects of appellant's invention as recited in the subject claims. Tucker *et al.* teaches a counting methodology for tracking object references in an object oriented computing environment. The method is concerned with reclaiming memory associated with object references that are no longer in use by applications. The cited reference discloses a door mechanism *for securing invocation of objects*. A door is a file descriptor that is protected from user-level forgery. The user level applications rely on an xdoor table that is mapped to the actual door for referencing secured objects. A handler routine performs the mapping so that an application can invoke the object. The Office

Action dated May 8, 2006 asserts that the file descriptor represents the message key and the handler represents the attribute. However, Tucker *et al.* fails to disclose a message key that is *part of an outgoing message* and is used for securing communications as in appellant's claimed invention. The subject invention includes a message key within each outgoing message. Tucker *et al.* employs the file descriptor to secure invocation of the object. Once an application has invoked an object, for example, a communication object, the application can send multiple messages that do not include any message keys. Furthermore, Tucker *et al.* is silent regarding *a filter associated with a communication component that controls sending of messages based upon the message key and one of the attribute conditions*. The filter of the subject claim employs the message key and the attribute condition in combination to determine if the message should be sent. The message key must be valid to allow sending of the message. The setting of the attribute condition determines what message key values are valid. For example a first setting of the attribute may mean a first set of message key values are valid and a second setting of the attribute may mean a second set of message keys are valid. The handler does not control the sending of *each message* based upon a message key in combination with an attribute. The handler merely controls invocation of an object based on a valid door identifier. The object that is called may send the outgoing message, but the cited art does not disclose that the object performs any validation. Thus, Tucker *et al.* does not teach or suggest that the outgoing message includes a message key having a key value, an attribute being associated with the communication component, the attribute having selectable attribute conditions that are inaccessible by the associated process; and a filter associated with the communication component, the filter controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions.

In view of the foregoing, appellant's representative respectfully submits that Tucker *et al.* fails to teach or suggest all limitations of the subject invention as recited in independent claim 1, (and claims 2 and 5-11 that depend there from), and thus fails to anticipate the claimed invention. Accordingly, reversal of this rejection is respectfully requested.

B. Rejection of Claims 12-15, 20, 25-27 and 29-33 Under 35 U.S.C. §102(b)

Claims 12-15, 20, 25-27 and 29-33 stand rejected under 35 U.S.C. §102(b) as being anticipated by Tucker *et al.* (U.S. Patent No. 5,808,911). It is respectfully submitted that this

rejection should be reversed for at least the following reasons. Tucker *et al.* does not teach each and every element of the subject invention as recited in the subject claims.

Independent claim 12 (and similarly independent claims 25, 29 and 30) recites *a first queue operative to store a request received directly from a first of the at least two processes and, upon validation of the stored request, to send the stored request to a second of the at least two processes, the stored request including a destination address and a key having a key value; and an interface operative to validate the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the first queue, the at least one key value associated with the first queue being unavailable to the first process.* Similar to the discussion above with respect to independent claim 1, Tucker *et al.* fails to teach or suggest validation of a request from a first process to a second process that is stored in an intermediate queue based upon a key value in the request and one or more key values associated with the queue. The cited art does not teach or suggest that a destination address and a key value are stored within the request. Rather, the cited reference relies upon a mapping in the xdoor table to secure an object call. The object call contains an xdoor identifier that is mapped to a door identifier to complete the object call. Moreover, the cited art does not disclose that the handler sends the request. The handler invokes objects based upon valid door identifiers. An object may then send the request. Therefore, Tucker *et al.* fails to teach or suggest *the stored request including a destination address and a key having a key value; and an interface operative to validate the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the first queue, the at least one key value associated with the first queue being unavailable to the first process.*

In view of the foregoing, appellant's representative respectfully submits that Tucker *et al.* fails to teach or suggest all limitations of the subject invention as recited in independent claims 12, 25, 29 and 30 (and claims 13-15, 20, 26, 27 and 31-33 that depend there from), and thus fails to anticipate the claimed invention. Accordingly, reversal of this rejection is respectfully requested.

C. Rejection of Claims 3, 4 and 16-19 Under 35 U.S.C. §103(a)

Claims 3, 4 and 16-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Tucker *et al.* (USPN '911) in view of Neal *et al.* (U.S. Patent No. 6,766,467). It is respectfully

submitted that this rejection should be reversed for at least the following reasons. Tucker *et al.* in view of Neal, *et al.* fails to teach or suggest each and every limitation of appellant's claimed invention.

To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The subject claims respectively depend from independent claims 1 and 12. As noted *supra*, Tucker *et al.* does not teach or suggest each and every element of the subject invention as recited in these independent claims, and Neal *et al.* fails to make up for the aforementioned deficiencies of Tucker *et al.* Neal, *et al.* teaches a system and method for pausing a send queue without causing errors in other queues. Neal, *et al.* fails to teach or suggest any keys or attributes used for security of communications as recited in independent claims 1 and 12. Therefore, reversal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP185USB].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact appellant's undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROC & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin

Reg. No. 40,894

AMIN, TUROC & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A system to facilitate secure communication, comprising:
a communication component operative to store an outgoing message received directly from an associated process, the outgoing message including a message key having a key value, an attribute being associated with the communication component, the attribute having selectable attribute conditions that are inaccessible by the associated process; and
a filter associated with the communication component, the filter controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions.
2. The system of claim 1, wherein the communication component further comprises at least one storage device operative to store messages.
3. The system of claim 2, wherein the at least one storage device further comprises at least one queue operative to store messages being sent by the associated process.
4. The system of claim 3, wherein the at least one queue further comprises at least two queues, one of the at least two queues being operative to store messages being sent by the associated process and another of the at least two queues being operative to store messages being sent to the associated process.
5. The system of claim 1, wherein the message key corresponds to a key associated with another communication component that is associated with a desired destination.
6. The system of claim 1, wherein the message key is a multi-bit field for storing data identifying a key associated with a destination communication component.
7. The system of claim 1, wherein the filter is operative to prevent sending the outgoing message from the communication component upon detecting an invalid message key in the outgoing message.

8. The system of claim 7, wherein key data having a range of at least one key value is associated with the communication component, the key data being inaccessible by the associated process, the filter controlling transmission of the outgoing message based on the validation of the message key as a function of one of the attribute conditions and the range of at least one key value.
9. The system of claim 8, wherein the filter employs the attribute to define a valid range of at least one key value based on the at least one key value associated with the communication component, such that the filter provides different control in connection with a message having a message key within the valid range and a message having a message key outside the valid range.
10. The system of claim 9, wherein the key data identifies a plurality of key values.
11. The system of claim 10, wherein the filter is operative to permit whether a message having a message key in the valid range is sent from the communication component.
12. A system to facilitate secure communication between at least two processes, comprising:
 - a first queue operative to store a request received directly from a first of the at least two processes and, upon validation of the stored request, to send the stored request to a second of the at least two processes, the stored request including a destination address and a key having a key value; and
 - an interface operative to validate the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the first queue, the at least one key value associated with the first queue being unavailable to the first process.
13. The system of claim 12, further comprising an attribute associated with the first queue, the attribute defining a valid range of key values based on the at least one key value associated with the first queue to control sending stored requests from the first queue.

14. The system of claim 13, wherein the attribute has selectable attribute conditions that are unavailable to the first process and the valid range of message keys varies as a function of the attribute conditions and the at least one key value associated with the first queue.
15. The system of claim 14, wherein the at least one key value associated with the first queue further comprises a plurality of key values associated with the first queue and unavailable to the first process.
16. The system of claim 14, wherein the attribute is set to have one of at least a first condition and a second condition.
17. The system of claim 16, wherein the interface is operative to prevent the stored request from being sent from the first queue if the attribute has the first condition and the key has a value that agrees with the at least one key value associated with the first queue.
18. The system of claim 17, wherein the interface is operative to permit the stored request from being sent from the first queue if the attribute has the first condition and the key has a value that disagrees with the at least one key value associated with the first queue.
19. The system of claim 16, wherein the interface is operative to prevent the stored request from being sent from the first queue if the attribute has the second condition and the key has a value that agrees with the at least one key value associated with the first queue.
20. The system of claim 12, wherein the interface is operative to prevent sending the request from the first queue if the request includes an invalid key.

21. A system to facilitate secure communication between at least two user-level processes, comprising:

storage means for storing an outgoing message received from a first of the at least two processes, the outgoing message including a message key associated with a destination, an attribute being associated with the storage means, the attribute having selectable attribute conditions unavailable to user-level processes; and

control means for controlling sending of the stored outgoing message from the storage means based on the message key and one of the attribute conditions.

22. The system of claim 21, further comprising validation data associated with the storage means and unavailable to user-level processes, the control means controlling sending of the outgoing message based on the validation of the message key as a function of the attribute and validation data.

23. The system of claim 22, wherein the validation data comprises at least one key value.

24. The system of claim 23, wherein control means is operative to control whether the stored message can be sent from the storage means based on the message key relative to a valid range of key values, which varies as a function of one of the attribute conditions and the validation data.

25. A system to facilitate secure communication between at least two user-level processes, comprising:

storage means for storing a request received directly from a first of the at least two processes and, upon validation of the stored request, for sending the stored request to a second of the at least two processes, the stored request including a key having a key value; and

validation means for validating the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the storage means, the at least one key value associated with the storage means being unavailable to user-level processes.

26. The system of claim 25, further comprising an attribute associated with the storage means, the attribute defining a valid range of key values based on the at least one key value associated with the storage means, the validation means controlling sending stored requests from the storage means according to the valid range of key values.
27. The system of claim 26, wherein the attribute has selectable attribute conditions that are not available to user-level processes, the valid range of key values varying as a function of the attribute conditions and the at least one key value associated with the storage means.
28. A computer-readable medium having computer-executable instructions for:
- storing in a storage device an outgoing message received directly from an associated user-level process, the outgoing message including a message key having a key value, an attribute being associated with the storage device, the attribute having selectable attribute conditions unavailable to user-level processes; and
 - controlling sending the stored outgoing message from the communication component based on the key value of the outgoing message and one of the attribute conditions.
29. A computer-readable medium having computer-executable instructions for:
- storing a request received directly from a first of at least two user-level processes in a storage device;
 - upon validation of the stored request, sending the stored request to a second of the at least two processes, the stored request including a key having a key value; and
 - validating the stored request based on the key value of the stored request relative to at least one predetermined key value associated with the storage device, the at least one key value associated with the storage device being unavailable to user-level processes.

30. A method to facilitate secure communication from a first user-level process in a system in which the first process is operable to communicate directly with hardware, comprising:

storing an outgoing message received directly from the first process in an associated storage device, the outgoing message including a message key having a key value; and

controlling sending of the stored message to a second process based on the value of the message key relative to a predetermined at least one key value associated with the storage device, the at least one key value associated with the storage device being unavailable to the first process.

31. The method of claim 30, further comprising associating an attribute with the storage device that is operable to define a valid range of key values based on the at least one key value associated with the storage device, and controlling sending of the stored message from the storage device based on the message key thereof and the defined valid range of key values.

32. The method of claim 31, wherein the attribute has selectable attribute conditions not available to the first process, the valid range of key values varying as a function of the attribute conditions and the at least one key value associated with the storage device.

33. The method of claim 30, further comprising validating the message key relative to the at least one key value associated with the storage device, and, upon detecting an invalid message key, preventing the stored message from being sent from the storage device.

34. A method to facilitate secure communication from a first user-level process in a system in which the first process is operable to communicate directly with hardware, comprising:

storing an outgoing message received directly from the first process in a storage device associated with the first process, the outgoing message including a message key associated with a destination, an attribute being associated with the storage device, the attribute having selectable attribute conditions being inaccessible by user-level processes; and
controlling sending of the stored outgoing message from the storage device based on the message key of the stored outgoing message and one of the attribute conditions of the storage device.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.